WHAT IS CLAIMED IS:

1. A storage system comprising:

an interface to a host computer;

a storage controller including a central processing unit that conducts an I/O operation and management operation;

a memory to store an operation log, the operation log being used to record a description of a management operation and a corresponding timestamp;

storage volumes defined by at least one storage device; and

an attribute for each of the storage volumes stored in the memory,

wherein write access to each of the storage volumes is dependent on the attribute.

2. The storage system of claim 1 wherein the attribute identifies a storage volume as at least one of write protected, offline, and normal.

3. The storage system of claim 1 wherein the memory is a non-volatile random access memory.

4. The storage system of claim 1 wherein the storage device is a hard disk drive, the storage system having at least 10 hard disk drives, the storage system being a disk array unit.

5. The storage system of claim 1 further comprising a management interface connected to a console, the console receiving the operation log from the storage system.

6. The storage system of claim 5 wherein the management interface is further connected to the console via a communication network, wherein the console receives the operation log over the communication network.

7. The storage system of claim 1, wherein a write protect period is associated with each of the storage volumes identified by the attribute as write protected.

8. The storage system of claim 1 wherein the operation log comprises:

a first log for system management operations; and

a second log for logical volume operations.

9. The storage system of claim 8 wherein the second log comprises volume operations for each of the storage volumes depending on the attribute.

10. The storage system of claim 8 wherein the operation log further comprises an I/O operation log for recording read access information for each of the storage volumes.

11. A method of assuring genuineness of data maintained on a storage subsystem having a storage controller and a plurality of storage disks, the method comprising:

maintaining a first log and second log;

recording management operations of the storage subsystem and corresponding timestamps to the first log;

identifying a write protect attribute and write protect period for a logical volume;

recording management operations of the logical volume and corresponding timestamps to the second log depending on the write protect attribute and write protect period;

denying write access to the logical volume to a host based on the write protect attribute and write protect period of the logical volume; and

providing information from the first log, second log, or a combination of the first and second log to a console.

12. The method of claim 11 wherein the first log and second log are stored in non-volatile random access memory.

13. The method of claim 11 wherein the write protect attribute and write protect period are store in the non-volatile random access memory.

14. The method of claim 11 wherein the information is provided over a communication network to a user on the console.

15. The method of claim 11 further comprising:

specifying a threshold for sequential read access to the logical volume;

monitoring read access to the logical volume; and recording information and corresponding timestamp to the second log if the threshold is exceeded.

16. The method of claim 15 wherein the threshold applies to all logical volumes of the storage subsystem.

17. A computer program product stored on a computer-readable storage medium for assuring genuineness of data maintained on a storage subsystem having a storage controller and a plurality of storage disks, the computer program product comprising:

code for maintaining a first log and second log;

code for recording management operations of the storage subsystem and corresponding timestamps to the first log;

code for identifying a write protect attribute and write protect period for a logical volume;

code for recording management operations of the logical volume and corresponding timestamps to the second log depending on the write protect attribute and write protect period;

code for denying write access to the logical volume to a host based on the write protect attribute and write protect period of the logical volume; and

code for providing information from the first log, second log, or a combination of the first and second log to a console.

18. The computer program product of claim 17 further comprising:

code for specifying a threshold for sequential read access to the logical volume;

code for monitoring read access to the logical volume; and

code for recording information and corresponding timestamp to the second log if the threshold is exceeded.